UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/814,330	04/01/2004	Carl Rajsic	ALC 3124	5344

7590 12/13/2010

KRAMER & AMADO, P.C.
1725 Duke Street, Suite 240
Alexandria, VA 22314

EXAMINER	
MOORE JR, MICHAEL J	

ART UNIT	PAPER NUMBER
2467	

MAIL DATE	DELIVERY MODE
12/13/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte CARL RAJSIC

Appeal 2009-006982
Application 10/814,330
Technology Center 2400

Before KENNETH W. HAIRSTON, THOMAS S. HAHN, and BRADLEY W. BAUMEISTER, *Administrative Patent Judges.*

HAIRSTON, *Administrative Patent Judge.*

DECISION ON REQUEST FOR REHEARING[1]

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

In a Decision dated August 31, 2010, the Board affirmed the anticipation rejection of claims 1, 5, 7, and 9 to 13, and the obviousness rejections of claims 2, 3, 6, and 8. In the Decision, the Board also reversed the anticipation rejection of claim 4. Appellant has requested a rehearing of our decision to affirm the anticipation and obviousness rejections of claims 1 to 3 and 5 to 13 (Req. Reh'g. 1, 5).[2]

In the Decision, we determined the following (*see* Dec. 10-11):

(1) Hall explicitly or inherently discloses multiservice switches and a method, and computer program performing a method, for establishing a secure Layer-3 connection across an ATM network, as set forth in claims 1 and 10 to 13. Hall discloses "anticipated security information" (independent claims 1 and 10 to 13) and "configuring" (claim 1) or embedding an MSS with such information (claims 10 to 13). *See* Dec. 8-9; FF 2, 3.

(2) Hall does not teach the interlock codes set forth in claim 4. *See* Dec. 9-10; FF 4.

(3) Appellant has not shown the Examiner erred in rejecting claims 1, 5, 7, and 9 to 13 under 35 U.S.C. § 102(e) or claims 2, 3, 6, and 8 under 35 U.S.C. § 103(a). *See* Dec. 10-11.

(4) Appellant has shown the Examiner erred in rejecting claim 4 under 35 U.S.C. § 102(e). *See Id.*

---

[2] Appellant requests rehearing of the anticipation rejection of claims 1, 4, 5, 7, and 9 to 13 (Req. Reh'g. 1), and asks the Board to "reconsider its decision to affirm the rejections of claims 1-13" (Req. Reh'g. 5). Since our Decision reversed the anticipation rejection of claim 4 (Dec. 11), we will reconsider our Decision with regard to the anticipation rejection of claims 1, 5, 7, and 9 to 13, and the obviousness rejections of claims 2, 3, 6, and 8.

We have reconsidered our Decision of August 31, 2010, in light of Appellant's comments in the Request, and we find no errors therein. We therefore decline to change our prior decision for at least the following reasons.

In the decision, the Board provided some elucidation of the portions of Appellant's Specification related to the claimed "anticipated security information" and the configuring of the terminating MSS with that information:

> Appellant describes a method for securely establishing a Layer-3 connection using an ATM network 12 including originating multiservice switches (MSSs) (Spec. ¶¶ [01] and [02]). A setup message including security information is sent from an originating MSS 18 over an ATM network 12 to a terminating MSS 24 (Fig. 1). The security information may include a closed user group interlock code (Spec. ¶ [14). The terminating MSS 24 is configured with anticipated security information which can be a closed user group interlock code (Spec. ¶¶ [16], [17]; originally filed claim 1).

(Dec. 5; FF 1). Although the Board found in the original decision that Hall teaches away from using interlock codes as recited in claim 4 (Dec. 9), Hall's closed user group identifiers serve the recited function of "anticipated security information" as set forth in claims 1 to 3 and 5 to 13.

Appellant contends that the Decision misapprehends Appellant's argument that Hall fails to disclose "'configuring the terminating MSS with anticipated security information'" (Req. Reh'g. 2), because "Hall does not make use of, and is therefore not configured with, any anticipated security information" because "Hall retrieves all closed group identifiers" (Req. Reh'g. 3). We disagree, and note that Appellant admits "the Decision

correctly notes that the phrase 'only' does not occur in claims 1, 5, 7, and 9-13" (Req. Reh'g. 2).

As stated in the original Decision:

> The phrase "only" does not occur in claims 1, 5, 7, and 9 to 13, nor do these claims limit operations to just a subset or part of the security information. In our view, independent claims 1, and 10 to 13 do not encompass the concept of operating on *only* part of the security information. Inasmuch as Appellant's arguments in this regard are not commensurate with the language of the claims, this line of reasoning is not persuasive.
>
> We find that Hall discloses anticipated security information and embedded security information inasmuch as Hall's security information (i.e., closed user group identifiers for called parties and calling parties) performs the same function as Appellant's security information used for call setup and authorization for a Layer-3 connection in a closed user group over an ATM network (*compare* FF 1 *with* FF 2 and 3). The security information recited in claim 1 would be reasonably understood by one of ordinary skill in the art to encompass Hall's closed user group identifiers for called and calling parties because a call is authorized and established based on a check of the closed user group identifiers (FF 2 and 3).

(Dec. 8).

Similarly, Appellant's argument that Hall's closed group identifiers cannot be characterized as anticipated security information "because a call may be set up regardless of whether a matching pair of closed group identifiers is found" is unpersuasive (Req. Reh'g. 3) because Hall's blocks 526 and 530 in Figure 5 provide conditions where a call is not set up when no match of security information is found. In other words, Appellant's assertion that "a call may be set up even if matching closed group identifiers are not present" (Req. Reh'g. 3 (emphasis omitted) (citing Hall, Fig. 5,

reference characters 508, 512, and 522-532)) is incorrect, because Hall discloses at blocks 526 and 530 conditions upon which a call set up fails and is rejected when no closed user group identifier match is found.

Appellant also contends that the Decision misapprehends Hall's disclosure because the claimed subject matter performs a *different function* than Hall's closed group identifiers (Req. Reh'g. 4). Appellant asserts that the recited "anticipated security information" is used to verify received security information, thereby ensuring that a secure connection is being established and allowing for detection of possible security breaches (Req. Reh'g. 4). This line of reasoning is unpersuasive inasmuch as independent claims 1 and 10 to 13 do not recite verification, or ensuring against possible security breaches. Instead, we find that the claims at issue describe "*configuring* the terminating MSS with anticipated security information" (claim 1 (emphasis added)), determining whether embedded security information *matches* the anticipated security information (claim 1), *comparing* the embedded security information with the anticipated security information (claims 10 and 11), *storing* anticipated security information (claim 12), and *retrieving* anticipated security information (claim 13).

In our original decision, we found that Hall describes a method for establishing an SVC over an ATM network with closed user groups in the flowchart of Figure 5 (col. 18, l. 32 through col. 21, l. 37). Dec. 5; FF 2. Hall describes "using a database" to *store* the closed user group identifiers (col. 19, l. 50). We found that Hall describes *retrieving* closed user group identifiers to determine a *match* (e.g., when a closed user group identifier common to both the called and calling party is found in block 508) (Dec. 6; FF 3). Thus, Hall establishes a secure connection by configuring, storing,

retrieving, and matching closed user group identifiers (i.e., anticipated security information).

We have carefully considered the arguments raised by Appellant in the Request, but none of these arguments is persuasive that the original decision was in error. We find that Appellant has not shown the Board erred in finding that (i) claims 1, 5, 7, and 9 to 13 are anticipated by Hall, (ii) Hall discloses anticipated security information inasmuch as Hall's closed user group identifiers perform the same function as Appellant's security information, and (iii) the combination of Hall and the applied secondary references teaches or suggests "configuring the terminating MSS with anticipated security information" in sustaining the rejections of claims 2, 3, 6, and 8 under 35 U.S.C. § 103.

In summary, Appellant's request for rehearing has been granted to the extent that our decision has been reconsidered, but such request is denied with respect to making any modifications to the Decision.

REHEARING
DENIED

babc

KRAMER & AMADO, P.C.
1725 DUKE STREET, SUITE 240
ALEXANDRIA, VA 22314